UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 13-CR-120

PAUL D. CASE,

Defendant.

UNITED STATES' SUR-REPLY BRIEF

The United States of America, by its attorneys James L. Santelle, United States Attorney, and Benjamin W. Proctor, Assistant United States Attorney, hereby files its sur-reply brief to the defendant's "Reply to Government's Response to Defendant's Motion to Suppress Evidence" (Doc. #27.)

I. Procedural Summary

On November 6, 2013, the defendant, Paul Case, filed a motion to suppress evidence asserting that the search warrant affiant intentionally omitted material facts. (Doc. #21). On November 7, 2013, the defendant filed an "Amended Motion to Suppress" in which he made several minor changes to the initial motion. (Doc. #22.) Pursuant to the scheduling order, the United States filed its response in opposition to the motion on November 18, 2013. (Doc. #23.) In that response, the United States focused on Case's failure to meet the basic requirements necessary to justify a *Franks* hearing. On November 19, 2013, Case filed a "Second Amended Motion to Suppress" in which he made another change to the amended motion. (Doc. #24.) On December 31, 2013, Case filed a "Reply to Government's Response to Defendant's Motion to

Suppress Evidence," along with 10 new exhibits. (*See* Doc. #27.) On January 2, 2014, the United States filed a motion seeking leave to file a sur-reply brief. (Doc. #28.) That motion was granted by the Court on January 3, 2014. On January 6, 2014, Case filed a supplemental attachment to his reply brief. (Doc. #30.)

II. Introduction

In his reply brief, Case has gone to great lengths to characterize as shady the programs used by law enforcement in investigating the sharing of child pornography through peer-to-peer networks. He submitted several academic articles and other documents discussing many different types of peer-to-peer programs used by individuals to distribute child pornography, as well as various law enforcement tools used to catch and prosecute those individuals.[1] But, upon review, these materials do nothing to support Case's motion for a *Franks* hearing. Moreover, Case is far from the first defendant charged with child pornography offense to challenge law enforcement investigations using peer-to-peer programs. Courts around the nation have heard such challenges, often on Fourth Amendment grounds. Importantly, these courts have roundly rejected such challenges. *See e.g. United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) ("Borowy also argues that the use of a 'forensic software program' that is unavailable to the general public to confirm that the files contained child pornography rendered Agent Mitchell's conduct an unlawful Fourth Amendment search. We disagree. Borowy had already exposed the entirety of the contents of his files to the public, negating any reasonable expectation of privacy in those files. . . . Moreover, the hash-mark analysis appears to disclose only whether the files in the list that Agent Mitchell's keyword search returned were known child pornography." (internal

[1] As described in the search warrant affidavit, the peer-to-peer network at issue in this case is known as Ares. (*See* Doc. #23 Ex. B ¶¶10-11, 25-26.) As Case acknowledges, many of his exhibits focus on other peer-to-peer networks. (*See* Doc. #27 at 2.)

citations omitted)); *United States v. Stults*, 575 F.3d 834, 843-44 (8th Cir. 2009) (rejecting defendant's assertions that law enforcement agents' use of software to download child pornography files via peer-to-peer network from computer with IP address tied to the defendant, which was basis for the search warrant, violated the Fourth Amendment; and rejecting the defendant's assertion that the affidavit supporting the search warrant, which described the online investigation, lacked a finding of probable cause); *see also e.g., United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (holding that defendant had no expectation of privacy in his subscriber information that was obtained by law enforcement as part of the investigation, including his IP address and name, from third party service providers, where the defendant voluntarily transmitted such information to internet providers and enabled a peer-to-peer file sharing program on his computer, which permitted anyone with internet access the ability to enter his computer and access certain folders).

Case's challenge is slightly different than those in the cases cited above in that, while he appears to question the constitutionality of the investigation, he attempts to do so by trying to attack the veracity of the search warrant affidavit in light of the Supreme Court's decision in *Franks v. Delaware,* 438 U.S. 154 (1978). As explained in the United States' response brief, Case bears a very high burden. The sole issue before the Court is whether Case has made a "*substantial* preliminary showing" that the search warrant affidavit was false because the affiant deliberately omitted a material fact. The *deliberate* omission must be of a *material* fact, which, had it been included, would have negated a finding of probable cause that illegal materials would likely be found at the address listed in the warrant.

Nothing in Case's initial brief or reply brief calls into question the key facts underlying the finding of probable case. Nothing. All of the facts previously cited by the government

remain essentially undisputed. (*See* Doc. #23 at 9-10.) More important, he fails to articulate what *material* evidence he intends to produce at a *Franks* hearing that would establish the search warrant affidavit is intentionally misleading. And, to put the issues in perspective, the information in the search warrant was corroborated by evidence obtained after the execution of the search. (*See* Doc. #23 at 3 (discussing relevant facts).)

III. Analysis of New Assertions and Arguments

With the above in mind, the United States responds to the following new assertions and arguments raised in Case's reply brief.

- "Agent Ungerer admitted to Case's computer forensic expert that RoundUp ran unattended during the time which encompasses Count One of the Indictment." (Doc. #27 1-2.)

This assertion comes from the Second Amended Motion to Suppress (recited in the reply brief) wherein Case "corrected" his initial brief by changing the name of person from "Agent Kolocheck" to "Agent Ungerer." (*See* Docs. #24, 27.) The United States pointed out in its response brief that no such statement was ever made by "Agent Kolocheck." (Doc. #23 at 6.) Unlike Case, the government submitted an affidavit from the alleged source of the statement to support its assertion. (Doc. #23 Ex. C.) Now Case claims that it was "Agent Ungerer" who made this statement.[2] But it remains unclear how this statement supports Case's motion. It appears Case (not the actual declarant) is summarizing in one sentence a conversation between a task force officer and his computer expert, and then relying upon his own summary to craft an argument. In any event, as discussed below, the argument is meritless.

[2] Case is apparently referring to Milwaukee Police Department Detective Brant Ungerer, who is part of an FBI task force investigating child exploitation offenses. Detective Ungerer's background is discussed in the search warrant affidavit. (*See* Doc. #23 Ex. B ¶1.)

- "Of note, at no point in its Response does the Government contest that the program RoundUp ran unattended during the Government's surveillance of the Case computer." (Doc. #27 at 2.)

This statement is simply wrong. First, the United States' focused on Case's assertion that "Agent Kolocheck" said the program ran "unattended." As noted, this was never true. Moreover, the United States addressed this argument in its response brief. (Doc. #23 at 6-7.) Case's entire assertion that the program ran "unattended" (in the sense that no person was aware or involved "during the time which encompasses Count One of the Indictment") is confusing.[3] But more importantly, whatever Case may mean by using the word "unattended," it has no impact on the material facts in the affidavit setting forth probable cause to believe that evidence of child pornography would be found at Case's residence. (*See* Doc. #23 at 9-10.)

- "Retrospectively, a more precise way to describe the misleading use of the words "investigative" and "session" in the Affidavit would be to point out the failure of the affiant to advise the issuing magistrate that the investigation that identified the location and content of the Case computer, its owner's name, as well as its IP address, was *automated* as well as *unattended*." (Doc. #27 at 2.)

With the above sentence, Case appears to be altering the argument he made previously. But it makes no difference. Case again fails to indicate what specific sentences or paragraphs in the search warrant affidavit he is contesting. As previously noted, the word "investigation" appears several times and the word "session" does not appear at all. (*See* Doc. #23 at 7.) The search warrant affidavit describes the investigation, the files at issue, and how law enforcement identified "its owner's name, as well as its IP address." (*See* Doc. #23 Ex. B. ¶¶ 25-33.)

[3] As discussed in the United States' response brief, the affidavit addresses the nature of the investigation into peer-to-peer networks, including how files are identified and shared. It goes on to state that, in this investigation, it took more than 24 hours to download the identified files directly from the computer at the IP address tied to Case. (*See* Doc. #23 Ex. B ¶¶7-21, 25-27.) Agents obviously used computer programs in conducting this investigation – the investigation involves an online investigation into the sharing of child pornography files.

- "Case continues to assert that the failure to advise the issuing magistrate [judge] of the name and features of the Roundup made it *unlikely* that an issuing magistrate would ever question whether the use of this particular program violates the restrictions placed on law enforcement by *Kyllo v. United States*, 533 U.S. 27 [] (2001)." (Doc. #27 at 3.)

- "The failure to disclose in the Affidavit the identity of a law-enforcement-only program, whose capabilities include centralized real-time surveillance of millions of members of peer to peer networks, prevented the issuing magistrate [judge] from determining for himself whether such data-mining was in violation of the Fourth Amendment." (Doc. #27 at 4.)[4]

These related arguments are presented for the first time in Case's reply brief. But it is not an argument relevant to a *Franks* hearing, which calls into question the integrity of the search warrant affidavit and the finding of probable cause. Again, Case does not challenge the facts in the affidavit that a computer with an IP address unquestionably tied to Paul Case made child pornography files available through a peer-to-peer program. If Case believes that law enforcement's ability to download files made available for sharing via peer-to-peer networks qualifies as an unreasonable search under the Supreme Court's decision in *Kyllo v. United States*, that is a separate issue. Importantly, such challenges are not new, and courts around the country have considered and rejected these types of arguments. *See e.g., United States v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011) (unpublished) ("Moreover, Norman's argument that law enforcement used 'unique' software that was not available to the general public, and his reliance on *Kyllo v. United States*, 533 U.S. 27 [] (2001), are misplaced because, as noted, he had placed the contents of the folder the police searched into the public domain, thereby negating any reasonable expectation of privacy in the folder."); *United States v. Gabel*, 10-60168, 2010 WL 3927697 (S.D. Fla. Sept. 16, 2010) ("The Undersigned agrees with every other federal court to have addressed this issue, and finds that users of peer-to-peer networks do not enjoy a

[4] Case rephrases this general argument regarding the Fourth Amendment in several parts of his reply brief.

reasonable, objective expectation of privacy in the files they share."), *report and recommendation adopted*, 2010 WL 3894134 (S.D. Fla. Oct. 4, 2010), *aff'd*, 470 F. App'x 853 (11th Cir. 2012); *see also Borowy*, 595 F.3d at 1048; *Stults*, 575 F.3d at 843-44.

- "The failure to disclose the name and capacities of RoundUp prohibited a neutral and detached magistrate from knowing that the program's developers acknowledged "in fact, there is often no connection between what is observed on the network, and what is found in the search." (Doc. #27 at 5.)

This is another new argument by Case as it is based on a quotation from a document attached for the first time to Case's reply brief. (*See* Doc. #27 Ex. 5 at 4.) But it is unclear what Case attempts to achieve through this assertion. To the extent Exhibit 5 has any bearing on Case's *Franks* motion (which, as a general academic article regarding investigations on other peer-to-peer networks, is dubious), the portion referenced by Case appears to describe what these authors perceive as general challenges associated with investigative tools in prosecuting child pornography distribution offenses. Case conveniently omits the rest of the sentence, the entirety of which is repeated below:

> In fact, there is often no connection between what is observed [by law enforcement] on the [peer-to-peer] network, and what is found in the search: *users may delete files, or install new client software*. As a result it is challenging to prosecute for distribution of [child pornography] in the case that some [child pornography] is found during a warrant-based search, but it is not the same files that were requested and downloaded by [law enforcement] from that peer. . . .

(Doc. #27 Ex. 5 at 4 (emphasis added).[5]) In other words, it appears the authors are positing that it is helpful for prosecuting distribution offenses if the same illegal files downloaded during a law enforcement investigation are later found on the defendant's computer following execution

[5] There is of course much more to the discussion in that article, which is provided in full as an exhibit to the defendant's reply brief.

of a search warrant at the defendant's residence. This in no ways calls into question the veracity of the search warrant affidavit in this case. In fact, while Case admitted to law enforcement that he tried to delete the child pornography files on his computer by performing a "factory reset" about a month before the search warrant was executed (but after law enforcement conducted the online investigation), remnants of those same files described in the warrant affidavit were found by law enforcement on Case's computer following a forensic examination.

- "Failure to specifically mention the name of the program prohibited the issuing magistrate [judge] from asking the affiant the extent, if any, of the training he had on the software used to identify the computer allegedly operated by the defendant." (Doc. #27 at 6.)

With this assertion, Case appears to be challenging the training of the affiant, which is a new argument presented for the first time in Case's reply brief. Case ignores the fact that the affiant references his experience and training in the search warrant affidavit. For instance, paragraph 1 of the affidavit states in part: "I am charged with conducting investigations of violations of federal law including the receipt, possession, distribution, and production of child pornography. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with other members of the CETF regarding these matters." (Doc. #23 Ex. B ¶1). Moreover, the affidavit goes on to state: "The information supplied in this affidavit is based upon my investigation, and information provided and investigation conducted by other law enforcement personnel in this matter to date." (Doc. #23 Ex. B ¶3.) Case does not directly challenge the affiant's training, and he fails to explain how failing to list in the affidavit the "specific courses" taken by the affiant (Doc. #27 at 7) negates a finding of probable cause.

- "In fact, the only image that the agent actually saw prior to the issuance of the search warrant was its own library of known images of child pornography, which is incorporated in the suite of software known as RoundUp. (Exhibit 1:29 & 31)" (Doc. #27 at 7.)

This is a new assertion raised by Case as it is based on an apparent power-point presentation regarding "Investigation of the eDonkey Network/Roundup Emule Updates" included for the first time in Case's reply brief.[6] The assertion is flat wrong. In this case, as addressed in the search warrant affidavit, files of suspected child pornography were successfully downloaded by law enforcement from Paul Case's computer on November 24-25, 2012, through the Ares peer-to-peer network. The files were child pornography videos, and they were described in detail in the affidavit. (*See* Doc. #23 Ex. B at ¶27.) Case provides no support for his assertion that agents viewed only images from "its own library" prior to the search warrant being issued. His references to the "Exhibit 1:29 &31," which appear to be screen shots unconnected to this investigation, are not helpful.

- "The Affidavit misrepresents that affiant who conducted the covert online investigation. [sic] Affiant did not observe anything. Online Cover Employee 5023 (OCE-5023) did not identify a computer with files of investigative interest." (Doc. #27 at 9.)

This assertion is raised for the first time in Case's reply brief as it appears to be based on notes in the power-point presentation regarding "Investigation of the eDonkey Network/Roundup Emule Updates" attached to the reply brief as Exhibit 1. And, though not clear, it appears that Case is taking issue with the word "identified" in Paragraph 25 of the affidavit, which states in relevant part: "During this time, OCE-5023 identified a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download." (*See* Doc. #23 Ex. B ¶25.) This challenge is meritless. Case does not (and cannot) dispute that law

[6] As Case acknowledges, the power point attached as Exhibit 1 is intended for use "with a different peer-to-peer network, called the Donkey Network." (Doc.#27 at 2.) The peer-to-peer program at issue in this case is known as Ares.

enforcement agents were involved in an online investigation into the sharing of child pornography over the Ares peer-to-peer network, and "a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download" was located (identified) during that investigation. (*See* Doc. #23 Ex. B ¶25.) The affidavit goes on to describe how and when certain files containing child pornography were downloaded by law enforcement from a computer at IP address 174.102.233.53; the content of those files; and how law enforcement connected the computer at IP address 174.102.233.53 to the defendant. (*See* Doc. #23 Ex. B. ¶26-33.) The logs of the investigation, and evidence and confessions obtained following the search, are consistent with the assertions in the affidavit.

IV. Case's Potential Witnesses

What purpose would be served by holding a *Franks* hearing in this matter? Here, Case has put forward all of the evidence he believes necessary to prevail on his motion. (*See* Doc. #27 at 12 ["With all due respect to the Government, the defendant concluded fishing prior to its [sic] filing of the second amended motion to suppress and is ready for the 'meal' that advocates call a hearing."]) But, as discussed, the focus of any *Franks* hearing would be whether the movant has established that the search warrant affidavit was deliberately and materially false, and Case has fallen far short of making a "substantial preliminary showing" on any of the three factors necessary to obtain a *Franks* hearing. *See e.g.*, *United States v. Maro*, 272 F.3d 817, 821 (7th Cir. 2001) (quoting *Franks*, 438 U.S. at 155-56.)

Moreover, while Case indicates that he intends to call "one or more of RoundUp's developers, as well as her [sic] own two experts, Jerry Grant and Steven Odenthal" as his witnesses at a *Franks* hearing, (Doc. #27 at 12), it appears that none of these individuals has information relevant to a *Franks* inquiry. This is illustrated by the "Affidavit of Gerald Grant,"

which Case filed as a supplement to his reply brief on January 6, 2014. (*See* Doc. #30-1.[7]) According to the affidavit, Mr. Grant is an advisor to Case and has reviewed (or at least, was asked to review) the discovery provided in this matter concerning the investigation. (Doc. #30-1 ¶3.)

Nothing in Mr. Grant's affidavit speaks to the content of the search warrant affidavit at issue. While Mr. Grant believes it would be helpful to review a user manual and training material for "RoundUp" for cross-examination purposes, he provides no information that would indicate the search warrant affidavit was false. In other words, the prospective testimony of Mr. Grant would not support Case's motion to suppress evidence based on an alleged *Franks* violation.

CONCLUSION

The limited purpose of this sur-reply is to respond to some of the new arguments presented by Case in his reply brief.[8] Even with dozens of pages of additional documentation (none of which, except for the Affidavit of Gerald Grant, is directly related to this investigation), Case presents nothing to support his claim that the search warrant affidavit was materially and deliberately false. Therefore, based on the materials submitted, the United States respectfully requests that Case's motion to suppress evidence and request for a *Franks* hearing be denied.

[7] The reply brief includes no citations to Mr. Grant's affidavit.

[8] There are many other assertions in Case's reply brief with which the United States takes issue. But none speak to the mind of the affiant, or seriously challenge the material facts set forth in the affidavit giving rise to a finding of probable cause.

Dated in Milwaukee, Wisconsin, this 17th day of January, 2014.

JAMES L. SANTELLE
United States Attorney

By: s/Benjamin W. Proctor

BENJAMIN W. PROCTOR
Assistant United States Attorney
Benjamin Proctor Bar No.: 1051904
Attorney for Plaintiff
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: (414) 297-1700
Fax: (414) 297-1738
Email: benjamin.proctor@usdoj.gov